device. Once communication with the device is established, Applicant's invention performs the necessary translation or modification of the packets sent to/from the device to make them "compatible" with the currently attached network -- without actually changing the configuration of the device.

Applicants' solution to establishing communication with an incompatible or improperly configured device was to intercept packets transmitted from the device. . Applicants' provide three examples (of the many possible) of how packets can be intercepted: Proxy ARP Packet Interception, Promiscuous Mode Packet Interception, and DHCP Request Interception. (see pp. 19-20 of specification) In each case, the present invention intercepts packets, i.e. receives and processes packets, which are not intended for the nomadic router/translator and in fact are likely intended for a device or host (such as a router or gateway) which is not on the foreign network (thus, are incompatible). The concept of intercepting packets as claimed by Applicants, described in the specification, indicated by its plain meaning, and as understood by those skilled in the art is neither disclosed nor suggested by the references relied upon.

Egevang

Egevang is directed to solving the problem of IP address reuse and describes a strategy for Network Address Translation (NAT) which maps private IP addresses to public, routable IP addresses. This allows reuse of the private IP addresses, i.e. multiple hosts may have the same IP address so long as they are isolated from each other. For the router disclosed by Egevang to perform NAT, the packets must be explicitly addressed to it at the link layer. Otherwise, the packets will be dropped by the router. Any incompatible or improperly configured device will not "know" of that particular router's existence and therefore can not establish communication with the router in the first instance. The router does not intercept packets as described and claimed by Applicants.

Li et al. (U.S. Pat. No. 6,012,088)

Li et al. is directed to solving the misconfiguration problem in an entirely different manner than that disclosed and claimed by Applicants. In Li et al., a customer contacts the Internet access provider, such as an ISP, to determine the proper configuration for the customer.

The proper configuration is then stored in a configuration server. The customer's device contacts the configuration server to retrieve the previously established settings or configuration so that the newly added device is compatible with the customer's network. Again, there is no teaching or suggestion to intercept packets to establish communication with the incompatible device and then translate data when necessary to make the device "appear" compatible with the network and vice versa.

Norris (U.S. Pat. No. 5,557,748)

Similar to Li, Norris discloses a strategy to select a previously determined configuration from a list of configurations. If the device recognizes a particular configuration from its list of stored configurations, the corresponding network settings are used for subsequent communication over that network. If a recognizable configuration does not exist, the device is unable to communicate over the network. Again, there is no teaching or suggestion to intercept packets to establish communication with the device in the first place and then selectively translate data within the packets to allow the device to communicate over the network as disclosed and claimed by Applicants.

Johnson et al. (U.S. Pat. No. 5,539,736)

Johnson is similar in some respects to both Norris and Egevang, and is also distinguishable. Johnson discloses an interface (communications) processor which performs protocol translation to accommodate communication over dissimilar network architectures or protocols. Johnson indicates that the interface processor, "which initially does not know the specific format being used by the data, examines the data to identify its format." (Col. 2, ll. 40-42.) Johnson also states that ". . . the CP 312 determines in what format the data is received. This determination is made based only on the received data, that is to say, without advance knowledge." (Col. 4. ll. 53-55) Like Egevang, Johnson assumes that the device is compatible with the network at the link layer in that the device must send packets to the interface processor. If the device is incompatible with the network, the interface processor would never receive the packets and process them in the first place. Similar to the router in Egevang, if the device is unaware of the existence of the router/processor, the packets will be dropped. There is no teaching or suggestion in Johnson to intercept packets as disclosed and claimed by Applicants.

irrelevant

Is this in the claim?

how is this done in the claim?

Johnson is similar to Norris in that Johnson includes a known list of protocols which can be translated. When a protocol is recognized based on its data, an appropriate translation is performed for the destination device. However, if the packets are not compatible at the link layer, i.e. addressed to the interface processor, no translation can be performed.

Summary

The prior art relied upon by the Examiner fails to disclose or suggest the concept of intercepting packets to establish communication with an incompatible device and translate or modify subsequent packets to "appear" compatible to the network. Applicants respectfully submit that the currently pending claims are patentable over the prior art of record.

Respectfully submitted,

JOEL E. SHORT et al.

By _____

DAVID S. BIR
Reg. No. 38,383
Attorney/Agent for Applicants

Date: March 30, 2000

BROOKS & KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
Phone: 248-358-4400
Fax: 248-358-3351